Department of Homeland Security Daily Open Source Infrastructure Report for 5 December 2008

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

- The Jersey Journal reports that Kuehne Chemical in Kearny, New Jersey, has been cited and fined by the U.S. Occupational Safety and Health Administration for 33 worker safety and health violations, OSHA officials confirmed Tuesday. (See item **4**)
- According to Newsday, a virus attack crippled computer systems in Islip Town offices and at Long Island MacArthur Airport in New York for more than a week in November but did not compromise operations or security at the airport, officials said Monday. (See item **10**)

DHS Daily Open Source Infrastructure Report Fast Jump

Production Industries: Energy; Chemical; Nuclear Reactors, Materials and Waste; Defense Industrial Base; Dams

Service Industries: Banking and Finance; Transportation; Postal and Shipping; Information Technology; Communications; Commercial Facilities

Sustenance and Health: Agriculture and Food; Water; Public Health and Healthcare

Federal and State: Government Facilities; Emergency Services; National Monuments and Icons

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − [http://www.esisac.com]

1. *December 3, Midlands News Service* – (Nebraska) **Worker burned atop wind turbine.** A worker — alone some 260 feet in the air — suffered first-and second-degree burns when the wind turbine he was installing in northeast Nebraska caught fire after a small explosion, said a spokeswoman for Edison Mission Group, owner of the Elkhorn Ridge wind farm. The worker climbed down on his own to receive aid. Two workers were on the ground when the employee was injured, she said. The injured worker was flown to a medical center in Sioux City, Iowa. The worker is an employee of Vestas, a wind turbine manufacturer. A spokesman with that company said the incident was under investigation and details would be provided when they became available. The spokeswoman for Edison Mission Group said the worker was outside the

turbine in front of its nose when the explosion and fire occurred. It is not clear what caused the explosion or what burned, but the turbines do have lubricating oil inside, she said. She said the wind farm was scheduled to go online at the end of this month, but work at the site has been suspended while the incident is investigated.
Source: http://www.southwestiowanews.com/site/news.cfm?newsid=20212336&BRD=2703&PAG=461&dept_id=627131&rfi=6

2. *December 3, Orange County Register* – (California) **Fire authorities probe lack of water at gas fire site.** Problems with finding an adequate water source forced firefighters to call on outside reinforcements to battle a toxic fire that broke out Monday at an oil and natural gas facility on the Seal Beach Naval Weapons Station. The fire department at the base is preparing to launch an investigation into why the plant's fire plan did not appear to work as it should have, base officials said. The Orange County Fire Authority (OCFA) is investigating the cause of the fire. "There is supposed to be a water system in place and in operation," said a spokesman for the base. "We do know that what they were supposed to have out there did not work very well." Breitburn Energy Partners of Los Angeles, the operator of the plant, is required to submit a fire plan to the state Department of Oil, Gas, and Geothermal. Monthly tests of the facility's fire equipment also must be conducted and reported to the state, according to California code regulations. A Breitburn executive vice president said the facility is equipped with two fire hydrants but "it appears the fire department wanted more water than those could supply." He said Breitburn will touch base with the OCFA to ensure their on-site hydrants were working properly. The OCFA at about 1:20 p.m. Monday responded to a natural gas fire that erupted on Oil Island, which is embedded in the National Wildlife Refuge on the base. When firefighters arrived there was no water source for them to tap into, and water tenders were immediately called on scene, said a captain with the OCFA. Firefighters also had to draw seawater from surrounding marshlands to snuff out the flames, he said. Flames shot up nearly 30 feet during the peak of the incident until a valve was shut off to prevent an underground pipeline from feeding natural gas into the fire.
Source: http://www.ocregister.com/articles/fire-water-gas-2245900-oil-refuge

[Return to top]

Chemical Industry Sector

3. *December 4, WAFB 9 Baton Rouge* – (Louisiana) **Chemical leak near Exxon leads to small-scale evacuation on Chippewa St.** Baton Rouge firefighters and hazardous materials crews responded to a chemical leak near the Exxon plant around 1:30 p.m. Wednesday. The leak was not located on Exxon property. A tanker truck leaked hydrochloric acid onto about 300 yards of roadway along Chippewa Street. Firefighters closed a nearly half-mile stretch of Chippewa Street from Scenic Highway to Phlox Avenue and evacuated workers from a nearby business. Exxon officials closed the south gate to their facility as a precaution, a spokesman said.
Source: http://www.wafb.com/Global/story.asp?S=9452630&nav=0aWU

4. *December 3, Jersey Journal* – (New Jersey) **Kearny chemical firm fined for safety violations.** Kuehne Chemical in Kearny has been cited and fined by the U.S. Occupational Safety and Health Administration (OSHA) for 33 worker safety and health violations, including lapses that could lead to a toxic chlorine release, an advocate group and OSHA officials confirmed Tuesday. On November 10 and 14, OSHA issued citations to Kuehne for violating federal standards and assessed total penalties of $48,650, said officials with the New Jersey Work Environment Council (WEC), an alliance of 70 labor and community organizations. WEC has characterized Kuehne, which sits across the Hackensack River from Jersey City, as "the nation's most potentially hazardous chemical plant." The OSHA violations include Kuehne's failure to: secure one-ton containers of liquid chlorine on forklift trucks to prevent them from falling off; accurately map potentially hazardous processes involving chlorine; assess the potential of pipe erosion/corrosion, which could cause a chlorine leak; and evaluate potential health effects on employees due to control failure.
   Source:
   http://www.nj.com/hudson/index.ssf/2008/12/kearny_chemical_firm_fined_for.html

[Return to top]

Nuclear Reactors, Materials, and Waste Sector

Nothing to report

[Return to top]

Defense Industrial Base Sector

5. *December 4, StandardNET* – (Nebraska) **Aging aircraft with maintenance issues carry military's advanced electronic equipment.** Poor maintenance may be compromising the flight safety of reconnaissance aircraft carrying some of America's most advanced electronic equipment, according to current and former aircraft mechanics. The RC-135 aircraft are maintained at Offutt Air Force Base in Nebraska and fly global intelligence-gathering missions. Top Air Force officials said that the 29 planes are properly maintained. But a senior civilian aircraft mechanic at Offutt with more than 30 years experience told the Kansas City Star that he has been waging a years-long battle to bring maintenance concerns to light about the RC-135 fleet and became so frustrated that he decided to go public. "I have found inspections that are 17 years past due, hydraulic and fuel hoses that should have been changed 15 years ago, and recently several emergency system hoses that were 30-plus years past time change," he said, adding that he believes at least one landing gear assembly also was improperly installed. Those concerns are backed by eight other current and former Offutt mechanics, and have sparked several congressional investigations into safety issues, plus an ongoing inquiry into whether the mechanic was disciplined for speaking out. The mechanic and other aircraft experts told the Kansas City Star that the maintenance issues are serious and could eventually lead to mechanical failures on the RC-135s, delaying critical missions or endangering crew members' lives. Air Force officials acknowledged that the age of the planes presents unique maintenance

challenges, and that at least one recent in-flight incident caused a significant problem. But they said most of the mechanic's concerns have been addressed, are unfounded, or were determined to be unsubstantiated.
Source: http://www.standard.net/live/news/150216/

[Return to top]

Banking and Finance Sector

6. *December 4, Merced Sun-Star* – (California) **Feds arrest four on bank-fraud accusations.** Federal agents descended upon a used auto dealer in Merced, California, early Wednesday, making arrests and serving a search warrant linked to a bank fraud investigation. A combined force of nearly a dozen FBI and Immigration and Custom Enforcement agents raided Auto Expo USA, said a FBI special agent. Agents arrested four suspects according to a five-page federal indictment. The suspects operated a scheme to enable customers to obtain financing, even if they did not qualify, by preparing false financial documents and forwarding them to Valley First Credit Union. Federal investigators believe the suspects entered fictitious information on loan applications, including the names of employers for whom the customers did not work. The men also inflated the earning amounts of customers, in addition to creating fictitious earnings statements to reflect payments of wages by businesses that never employed the customers. Once the loan application and supporting documents were completed, they were submitted to Valley First by either the suspects or the customers, the indictment said.
   Source: http://www.mercedsunstar.com/167/story/578067.html

7. *December 3, Associated Press* – (New Jersey) **NJ man gets 12 years in bank fraud scheme.** A New Jersey man has been sentenced to 12 years in federal prison for his role in a scheme involving millions of dollars in fraudulent home equity and business lines of credit. At a sentencing hearing on Wednesday a U.S. District Judge also ordered the defendant of Palisades Park to make restitution of nearly $10.5 million. That amount represents the verifiable losses sustained by banks in northern New Jersey that did business with the defendant between February 2004 and November 2005. The defendant, who was president of American Macro Growth (AMG) in Palisades Park, was indicted in June 2007 along with four AMG employees and eight clients of the company. He was a fugitive until May of 2008, when he was arrested in Queens, New York. Prosecutors say the defendant and his employees conspired to defraud at least 16 different lenders, partly by submitting falsified income tax returns on behalf of clients. The defendant pleaded guilty in July to conspiracy to commit bank fraud.
   Source: http://www.nj.com/newsflash/index.ssf?/base/news-35/1228342456120040.xml&storylist=jersey

[Return to top]

Transportation Sector

8. *December 3, CNN* – (National) **Report: Pilots' holsters make guns vulnerable to**

accidental discharge. Government-issued holsters used by thousands of armed airline pilots increase the chance that guns will be accidentally discharged in the cockpit, according to federal investigators. The holsters' design renders guns vulnerable to accidental firing if they are improperly handled, and should be replaced, said investigators who studied an incident in March in which a pilot discharged his weapon. They said the Transportation Security Administration (TSA) should provide a safer way to secure firearms in the distracting, sometimes dark environment of a cockpit. The TSA has defended the locking holsters, saying pilots have handled the holsters "millions of times" without incident since the holsters were put into service two years ago. But the Office of Inspector General — an independent arm of the Department of Homeland Security — concluded the design of the locking holsters "increases the likelihood of an accidental discharge of a weapon in an aircraft cockpit." The weapon also can be discharged if the pilot inserts the padlock hasp into the holster incorrectly, the report says. The TSA on Tuesday reiterated its statements that the holsters are safe. The Inspector General's recommendations on holsters were included in a semiannual report to Congress released this week.
Source:
http://edition.cnn.com/2008/TRAVEL/12/02/tsa.holster/index.html?iref=mpstoryview

9. *December 3, Los Angeles Times* – (California) **Red light Metrolink train ran before Chatsworth crash may not have been clearly visible.** A critical red light that a Metrolink train ran just before slamming into a freight train in Chatsworth was not as visible as green and yellow signals displayed by the same trackside warning device, investigators probing the disaster have found. The clarity of the stop light, as well as possible violations of communication rules by the commuter train's crew, have become key focus points in the federal inquiry into the deadliest rail accident in modern California history. "It was the unanimous consensus of the investigative team that the red was not as illuminated or clear or clearly lit," said one knowledgeable source. Most public attention after the crash, which killed 25 and injured 135, focused on dozens of cellphone text messages received and sent by the Metrolink engineer. One message was sent only 22 seconds before his train rammed into a Union Pacific freight train. It is unclear if a signal problem would reduce his potential responsibility for the crash. National Transportation Safety Board officials note that train collisions normally have more than one cause. Another part of the Chatsworth probe is zeroing in on a possible violation of a decade-old communication procedure intended to prevent signal-running collisions. Engineers are required to call out via radio all signal colors and their locations as they become visible. Conductors, who typically ride several cars away from the engineer, are required to confirm all yellow or red signals. Announcing and acknowledging signals over the radio serves as an extra safety check for crew members, and it also alerts nearby trains that another vehicle is in the area, experts say.
Source: http://www.latimes.com/news/local/la-me-metrolink3-2008dec03,0,1876430.story

10. *December 2, Newsday* – (New York) **Virus hits Islip Town, MacArthur Airport computers.** A virus attack crippled computer systems in Islip Town offices and at Long Island MacArthur Airport for more than a week but did not compromise

operations or security at the airport, officials said Monday. The disruption, which began November 20 and affected e-mail, individual hard drives, and town-wide servers, should be resolved December 2, the town information management director said. The attack, which officials estimate cost the town more than $50,000, underscored the need to upgrade the town's outdated technology, the Islip supervisor said. The computer systems "were someplace back in the late '70s when we came into office" in 2006, the supervisor said. "This year we're furiously advancing our systems to bring us at least into the 1990s." A new $270,000 operating system was in the testing phase when the virus hit, and its adoption may be delayed by the attack, the town information management director said. The Sality virus disabled virus protection software, then raced through the town's systems, shutting down 50 servers and infecting computers at facilities including Town Hall, Brookwood Hall, and MacArthur Airport. Within a day, it disrupted such activities as tax collection, code enforcement, and the issuing of permits and licenses. MacArthur was up and running Monday, the director said. Islip has reported the attack to Suffolk police and the district attorney's office, the Islip supervisor said, and the town's technology staff has been installing new security measures. MacArthur Airport is managed by the town and operates on two networks: one shared with Islip and one that is independent. The virus struck both, but technology staff managed to disconnect the independent network before much damage was done, the Islip supervisor said. No server data were lost, he said, although some individual hard drives lost files.
Source: http://www.newsday.com/news/local/suffolk/ny-limaca025949156dec02,0,1644211.story

[Return to top]

Postal and Shipping Sector

11. *December 2, Philadelphia Daily News* – (Pennsylvania) **News, meds, invites lost in alleged mail fiasco.** On Monday, dozens of customer complaints of delayed or missing mail poured into the Philadelphia Daily News in response to a front-page story documenting severe mail backlogs this year at the chronically understaffed U.S. Postal Service processing plant in Southwest Philadelphia. The story described how senior managers allegedly ordered the daily mail count to be falsified by undercounting items by the hundreds of thousands, as overflowing unsorted-mail bins multiplied on the plant floor, and trailers of unsorted mail were routed to other processing plants, only to return for sorting days later. Sometimes mail was destroyed in wake of the severe staffing shortages — which occurred as a result of a yearlong ban on overtime, say employees, put in place by managers who received performance bonuses.
Source:
http://www.philly.com/dailynews/local/20081202_News__meds__invites_lost_in_alleged_mail_fiasco.html

[Return to top]

Agriculture and Food Sector

12. *December 3, U.S. Food and Drug Administration* – (National) **FDA, EPA and USDA conclude that accidental release of genetically engineered cotton poses no safety risk to humans or animals.** The U.S. government announced Wednesday that there is no food or feed safety concern from an incident in which a small portion of an unauthorized genetically engineered (GE) cotton variety was harvested along with commercially available GE cotton. The U.S. Food and Drug Administration, the U.S. Environmental Protection Agency (EPA), and the U.S. Department of Agriculture's (USDA) Animal and Plant Health Inspection Service are working together following notification by the Monsanto Company that a small amount — less than an acre — of an unauthorized GE cotton variety was harvested along with 54 acres of a commercially available GE cotton variety. This unauthorized GE cotton variety produces a pesticide that is a plant-incorporated protectant. USDA has determined that the unauthorized GE cotton poses no plant pest concerns. The U.S. government is investigating whether a small amount of meal from the unauthorized GE cotton variety may have been inadvertently released into the animal feed supply. It is important to note that it has not been determined whether unauthorized cottonseed meal actually entered the feed supply. The processor is holding potentially affected material (both processed and unprocessed) pending further investigation. While EPA has concluded that consuming small amounts of the cottonseed poses no food or animal feed safety risks, under that Agency's LLP policy, the presence of this material in food or feed would be illegal.
Source: http://www.fda.gov/bbs/topics/NEWS/2008/NEW01920.html

[Return to top]

Water Sector

13. *December 4, Florida Today* – (Florida) **2 cities negotiate on water capacity.** West Melbourne leaders, weary from development delays, want to allow their own staff to determine whether enough water is available for new development. However, its water supplier, the city of Melbourne, is concerned its water system could be harmed if it does not do its own check on developments in neighboring West Melbourne. West Melbourne agreed this week to delay making changes to the plan that guides the city's future growth while it reviews until December 16 a compromise proposal Melbourne offered. The compromise allows West Melbourne to perform its own analysis, but also requires a review by Melbourne before a development could go ahead. The other option, Melbourne's city attorney said, would put off the concurrency issue until the two cities resolve ongoing water issues, now under court-ordered mediation. In exchange, Melbourne would hold off on its own proposed comprehensive-plan changes that would require West Melbourne to use its concurrency system. Melbourne's deputy city manager told West Melbourne City Council that his city needs to review how much water a new development requires to make sure its demands does not hurt Melbourne's system. Part of the problem, he said, is fire protection. The high flow needed during a fire fight could cause drops in water pressure for other customers in the Melbourne and beachside, causing boil water notices or even pipes to break. A fire in West Melbourne has never created that scenario, but it has happened in other parts of Melbourne's water system, he said.

Source:
http://www.floridatoday.com/article/20081204/NEWS01/812040318/1006/news01

14. *December 4, Baltimore Sun* – (Maryland) **Cause of 39th Street water main leak still unknown.** Baltimore City public works personnel have been trying to identify the source of a water main leak on 39th Street between St. Paul Street and Greenmount Avenue and repair it so the road can be reopened to traffic, a spokesman said Thursday morning. Mechanical failure at a nearby pumping station caused a surge of water that led to leaks at several joints, 12 feet apart along the 42-inch main underneath 39th Street, said a spokesman for the city Department of Public Works. DPW workers dug 15 feet down to the pipe, but the "leak is so small we have not been able to detect it," he said. A contractor will use sound equipment to locate the leak, he said. Once they pinpoint its location, personnel will backfill the existing hole and dig at that site, he said.
Source: http://www.baltimoresun.com/news/local/baltimore_city/bal-watermain1204,0,6985166.story

15. *December 3, U.S. Environmental Protection Agency* – (National) **Agencies revise guidance to protect wetlands and streams.** The U.S. Environmental Protection Agency (EPA) and the Department of the Army are issuing revised guidance to ensure America's wetlands, streams, and other waters are better protected under the Clean Water Act (CWA). The guidance clarifies the geographic scope of jurisdiction under the CWA. The revised guidance replaces previous policy issued in June 2007 and clarifies a June 2006 Supreme Court decision in Rapanos v. United States regarding the scope of the agencies' jurisdiction under the CWA. The guidance follows the agencies' evaluation of more than 18,000 jurisdictional determinations and review of more than 66,000 comments.
Source:
http://yosemite.epa.gov/opa/admpress.nsf/0/da22ecd8b385087285257514006a2bef?OpenDocument

16. *December 3, WMDT 47 Salisbury* – (Delaware) **Mispillion River reopens after sewage spill.** The Mispillion River reopened Wednesday after the public works department decided to drain over 1 million gallons of raw sewage into it between Monday and Tuesday. A broken sewage pipe caused a mess in front of the I.G. Burton dealership in Milford, Delaware, on Monday. A PIO says, "Corrosion happens to pipes, it is underground and we have no way of predicting when these things are going to happen." County officials say they had two choices — they either had to let the sewage run up through the manholes in the City of Milford, or send it to the river. Officials decided it was best for residents' health and drivers' safety to send it to the river. About 1.5 million gallons of raw sewage had drained into the Mispillion River. While State officials agree the county did not have many options, they say they are investigating and fines are possible.
Source: http://www.wmdt.com/topstory/topstory.asp?id=4008

[Return to top]

Public Health and Healthcare Sector

17. *December 4, Ventura County Star* – (California) **Computer equipment taken from medical company.** Computer equipment was stolen Sunday night from an Oxnard office that collects patient samples for medical testing, a company official confirmed Wednesday. Quest Diagnostics Patient Service Center had a break-in and theft of “non-data-storing computer equipment,” said a representative for the lab company, based in New Jersey. The Oxnard location is not a laboratory, she said. The center, which collects blood and urine samples from patients, was closed at the time, and no employees were present, she said. “We are confident that patient health information and other Quest Diagnostics’ data was not affected by this incident and continues to be secure,” she said in an e-mail. She would not provide any further information about the computers. The Oxnard Police Department is investigating the incident, she said.
Source: http://www.venturacountystar.com/news/2008/dec/04/computer-equipment-taken-from-medical-company/

18. *December 3, Health Day News* – (International) **Report confirms source of contaminated heparin.** A final report on the deadly contamination of the blood thinner heparin confirms that the problem was caused by a man-made chemical that was added to batches of the drug imported from China, U.S. investigators report. The crisis, which began last November, resulted in 152 adverse reactions and as many as 81 deaths in the United States. The Chinese heparin, contaminated with the chemical oversulfated chondroitin sulfate, was found in at least 10 countries, according to federal officials. “The last case was reported on January 31,” said a medical epidemiologist with the U.S. Centers for Disease Control and Prevention, and a member of the investigation team that wrote the report. Published in the December 4 issue of the New England Journal of Medicine, the report “describes the adverse reactions caused by the contaminant” and links it to a specific substance. The reactions included a drastic drop in blood pressure, nausea, and shortness of breath, starting within 30 minutes after the administration of the heparin.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2008/12/03/AR2008120302758.html

[Return to top]

Government Facilities Sector

19. *December 3, Ocala Star-Banner* – (Florida) **Man charged with planting ‘hoax bomb’ at jail.** At 9:05 a.m. Wednesday, exactly 12 hours after the Sheriff’s Office Bomb Squad exploded a suspicious outside the Marion County Jail, the unit had to do the same thing all over again. Meanwhile, deputies arrested a 31-year-old man in connection with the first incident and charged him with planting a hoax bomb. Sheriff’s officials said the second package, a brown box, was discovered Wednesday morning by a trash can at the entrance of the agency’s Operations Center. The Bomb Squad deployed Remo-Tech to the package, and the robot picked it up and moved it to a safe location at a retention pond. The robot then blew up the package at 9:05 a.m. It

contained mostly paper. Deputies believe this package may be connected to the other suspicious package that was thrown against a jail fence Tuesday night. Deputies released video images of a man, who looks like the defendant, leaving the second package by the front door of the Sheriff's Office.
Source:
http://www.ocala.com/article/20081203/ARTICLES/812030287?Title=Bomb_Squad_blows_up_second_box__man_arrested

[Return to top]

Emergency Services Sector

20. *December 3, Associated Press* – (National) **Homeland chief advises successor not to reorganize.** The current Homeland Security Secretary advised his successor Wednesday not to reorganize the young Department or try to please everyone. He pointed to the recent terror attacks in Mumbai, India, as a reason not to make drastic changes to the Department, which was formed by combining multiple existing agencies in 2003 in response to the September 11th attacks. During a speech at Johns Hopkins University Wednesday evening, he cited reports that firefighters, law enforcement, military officials, and emergency managers in Mumbai were not coordinated when they responded to last week's attack. "Emergencies don't come neatly packaged in stovepipes," he said, addressing the argument by some groups that the Federal Emergency Management Agency should be removed from the Department because FEMA's mission is to respond to natural disasters and the Department's main mission is to prevent terrorist attacks. He argued that when different agencies plan and train together they are better suited to respond to disasters of all varieties.
Source:
http://www.google.com/hostednews/ap/article/ALeqM5jffjiY2QqyLRdFtvyWNb18XVr7pQD94RL6780

[Return to top]

Information Technology

21. *December 4, VNUNet* – (International) **Sun and VMware issue vital updates.** Users are being advised to update their software after Sun Microsystems and VMware posted software fixes Wednesday. The patch from Sun addresses security and stability problems in Java, fixing 18 flaws covering stability, data corruption, and security vulnerabilities. Sun did not provide details on the exact nature of the security flaws, but the U.S. Computer Emergency Response Team has advised users and administrators to install the Java update immediately. The VMware patch, meanwhile, addresses two security flaws in a number of the company's virtualisation products. The fix applies to VMWare Workstation versions 5 and 6, VMWare Player versions 1 and 2, and VMWare Server version 1.0.9 and earlier, as well as the company's ESX offering. The first of the two flaws addresses a problem which could allow an attacker to remotely cause a memory corruption issue. If exploited, the attacker could cause the target system to crash and gain the ability to write code to memory. The second addresses a

previously patched flaw in the bzip2 library on ESX systems. If exploited, the vulnerability could be targeted by an attacker to crash the system while decompressing a specially-crafted archive file.
Source: http://www.vnunet.com/vnunet/news/2231942/sun-vmware-issue-updates

22. *December 4, VNUNet* – (International) **Secunia study finds 98 percent of PCs vulnerable.** A survey of computer users has shown that almost every PC is running at least one unpatched application, according to vulnerability testing firm Secunia. Secunia gathered reports from over 20,000 computer users who had downloaded its Personal Software Inspector tool, and found that over 98 percent have at least one application running that is vulnerable to attack. The company warned that the results are even more worrying since the tool is likely to have been downloaded predominantly by more security aware computer users. "Has the world improved since the last look at the numbers? The short answer is no. Nearly every PC continues to run with several insecure programs. If anything, these numbers are worse than [11 months ago] when we generated them initially," said Secunia. "The total number of PCs/users included in these numbers is 20,000, and 98.09 per cent have one or more insecure programs installed on their PC. Hence 98 out of 100 PCs that are connected to the internet have insecure programs installed." Another shocking figure from the research is that nearly 50 percent of PCs have 11 or more unsecured programs running on their computers. Secunia warned that antivirus software is largely ineffective at protecting against such vulnerabilities.
Source: http://www.vnunet.com/vnunet/news/2231922/secunia-study-finds-per-cent

23. *December 4, DarkReading* – (International) **Popular home DSL routers at risk of CSRF attack.** Researcher demonstrates ease of hacking home routers with insidious cross-site request forgery (CSRF) attack. A deadly attack typically associated with Websites can also be used on LAN/WAN devices, such as DSL routers, according to a researcher who this week demonstrated cross-site request forgery (CSRF) vulnerabilities in devices used for AT&T's DSL service. A consultant and founder of security think-tank Hexagon Security Group discovered a CSRF vulnerability in the Motorola/Netopia 2210 DSL modem that, among other things, could let an attacker insert malware onto the victim's computer or recruit it as a bot for a botnet. "CSRF is one of the only vulnerabilities that can be either completely innocuous or completely devastating," he says. The vulnerability is not isolated to Motorola/Netopia DSL modems. It affects most DSL modems because they don't require authentication to access their configuration menu, he says. "I can take over Motorola/Netopia DSL modems with one request, and I can do it from MySpace and other social networks," he says. The attack uses HTTP POST and GET commands on the modems, he says. CSRF vulnerabilities are nothing new; they are pervasive on many Websites and in many devices.
Source:
http://www.darkreading.com/security/vulnerabilities/showArticle.jhtml;jsessionid=DQEKHUYSQKAMSQSNDLPSKHSCJUNN2JVN?articleID=212201777

Internet Alert Dashboard

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: http://www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Communications Sector

Nothing to report

[Return to top]

Commercial Facilities Sector

Nothing to report

[Return to top]

National Monuments & Icons Sector

Nothing to report

[Return to top]

Dams Sector

Nothing to report

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports – The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open–source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421
Subscribe to the Distribution List:	Visit the DHS Daily Open Source Infrastructure Report and follow instructions to Get e-mail updates when this information changes.
Removal from Distribution List:	Send mail to NICCReports@dhs.gov or contact the DHS Daily Report Team at (202) 312-3421 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282–9201.
To report cyber infrastructure incidents or to request information, please contact US–CERT at soc@us–cert.gov or visit their Web page at www.us–cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non–commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.